Published and Copyright (c) 1999 - 2016
All Rights Reserved

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1803 01/15/16

~ Microsoft Collects MORE ~ People Are Talking! ~ Firebee Update News!
~ Gatekeeper Flaw Remains ~ Sharing Personal Info? ~ ATM Hackers Arrested!
~ Amiga OS Source Leaked? ~ Snoop Dogg to Gates! ~ UPP! for Atari 2600!

~ Hackers Cause Blackout! ~ SJC To Hear Xbox Case! ~ Seagates 10TB Drive!

-* Microsoft Fixes Critical Flaws! *-
-* The Dark Web's First Major News Site *-
-* Trend Micro Patches Password Manager Bug! *-

=~=~=~=

->From the Editor's Keyboard "Saying it like it is!"
"""""""""""""""""""""""""""""

It's been getting colder around here in New England, but more importantly, there's no (okay, a little) snow on the ground! Thankfully, oil prices have dropped significantly lately, so heating oil prices are dropping like the temperature!

Just looking at this week's batch of articles, I noticed a trend that was disturbing - most articles this week were about hackers, hackings, software flaws, and similar topics that do not give one that warm, fuzzy feeling.

It's obvious (or should be!) that today's technology - as it grows and improves - is an invitation for someone to hack into it and wreak havoc. Just look at the "power" that some of these hackers have these days: break into ATMs and steal money, cause massive power outtages, and the like. Upograde your PC to Windows 10 and open yourself to having Microsoft track what you do and where you do it! And most of the time, you don't have a single clue. And it's only going to get worse!

Until next time...

=~=~=~=

FireBee Update News

By Fred Horvat

Something I discussed in an earlier article was that I was going to try and setup the FireBee the best I could as a day to day machine. One of the tasks I mentioned was Backups. Well with the recent issues with the FireBee having issues not always booting successfully after the DIP Switch experiment. I figure I better get a good backup of my good running FreeMiNT setup that I have been working with over the past several months. This is currently on an 8GB CF card and all software installed on it has been tested good and configured (I believe) properly. So to lose all this work really would be very bad for me. I did a backup after I installed

and got working NVDI 5 but that was a couple of months ago and I never tested the backup. Without testing a backup you really can t say for sure that your effort has been worthwhile. How does one test a backup? To me it is to get that backup restored on a blank drive and back running properly. I was not going to backup my good 8GB CF Card and wipe it clean and restore it back though I was very confident that it would work. I had a second 8GB CF Card that I partitioned and formatted like my working one and restored to that CF Card.

There are a couple of different ways I could have done the backup and restore. The method I ended up using was not the first choice either. This is what I did that worked for me. First a description of the 8GB CF Card as this will help knowing what I was dealing with and the method I chose will make more sense. The 8CF CF Card is partition as one 990MB FAT16 Boot Partition containing FreeMiNT and one more FAT32 Partition of the remaining space of approximately 7GB that contains all my programs and user data (about 200MB of actual data). My first choice would have been to use a USB Flash Thumb Drive. Why I didn t chose it was that even though I have had the FireBee for about 6 months now I never plugged a USB Thumb Drive into the machine. So until I actually use one on the FireBee I was not going to rely on it. In all honestly I probably have nothing to even worry about but again I never used a Thumb Drive on the FireBee so I decided to go with what I have been using the whole time. That would be a SD Card in Drive A:. I grabbed a FAT16 formatted 1GB SD card and put in the FireBee and turned the FireBee on. I booted into FreeMiNT (which I do 99% of the time). I then created two folders on the SD Card. One folder called DriveC and another called DriveD. Then from the desktop I opened Drive C: and selected all files and folders on the drive and copied them to the DriveC folder on the SD Card. I did the same for Drive D: to the DriveD folder. I don t know exactly how long it took for each drive partially because once I started I walked away and came back a bit later. A few minutes for Drive C: and maybe 10-15 for Drive D:. I then shut down the FireBee and removed the 8GB CF Card and put in the newly prepared 8GB CF Card and booted into FireTOS. I reversed the process and copied the contents from the SD card DriveC to the CF C: partition. I rebooted into FreeMiNT so I had FAT32 support and then copied the DriveD folder to Drive D:. Time wise I didn t time it but it seemed to take longer or it felt that way because I was monitoring it more than before. After it was all done I removed the SD Card and rebooted the FireBee and booted into FreeMiNT. I ran a bunch of programs and all appears to be running fine. I plan on leaving in the newly created CF Card for a couple of weeks to test it more thoroughly but so far it seems to be working fine. During this time I need to keep track of any changes I make so I duplicate them back to the main CF Card also.

This was actually quite a simple process with the FreeMiNT that is supplied with the FireBee. FAT16 and FAT32 have almost the same file formats with FAT32 having long file name support, larger partition sizes, and other enhancements over FAT16. In my situation the files I had on my FAT32 partition Drive D: did not have any long file names. Had this been the case I would have had to use a FAT32 formatted USB Thumb Drive. I will be testing USB Thumb Drives and maybe external USB hard drives in the near future. When I do I will report my experiences. Now had I been

running EasyMiNT then I don t believe I could have backed up the Unix ext2 formatted partition(s) like I did by just copying data to and back from a FAT32 formatted USB Thumb Drive. I won t know until I try but I believe that it will mess up file attributes. In the event I do finally get EasyMiNT installer working or decide to manually put together SpareMiNT onto the FireBee I will try copying back and forth to see what happens. I may have to use Unix commands (like DD or TAR) to backup/copy the data to a USB Thumb Drive FAT32 or even ext2 formatted. I m not the strongest Unix user but I do have some hands on Unix experience.

One benefit of copying data to a SD or USB Thumb Drive is that I brought the SD card to a Windows PC and copied those folders to that machine for having another backup on a Windows PC. Even another benefit of having the data on the Windows PC was that I Zipped the folders into smaller single files for each drive and uploaded them to my DropBox account. Now I have backups in multiple places.

Amiga OS Kickstart and Workbench Source Coded Leaked

Generation Amiga has reported today a tweet from Hacker Fantastic saying that the Amiga OS source has been leaked, including both Kickstart and Workbench. Looking at the @hackerfantastic s tweet, there is another user with the handle @TheWack0lian that offers a link to download the OS in a 130MB tar file which expands to 540MB of source code.

As far I could gather, Hyperion Entertainment, despite filing bankruptcy in January of 2015, still holds the rights to modify and distribute the Amiga OS. They even released on Dec 17th the Amiga OS 4.1 Final Edition as Digital download, in partnership with Cloanto.

Apparently the source code is really related to Amiga OS. The tar file name refers to OS 3.1 but folders from the source code refers to version 4, which could mean the source code is pretty much up to date.

The retro scene is used to have almost everything for free and the fact Amiga OS is one of the few examples that still need to be purchased can show different reactions from the community.

We would love to hear what you have to say about it, as we could probably see illegal versions of the OS being released in upcoming months.

AmigaOS 3.1 Source Code Leak - Official Statement

Hyperion Entertainment wishes a happy New Year 2016 everybody!

The days between last Christmas and New Year were actually clouded by the sad fact that the source code of AmigaOS 3.1 and additional content dating back to 1994 was published and widely spread

without permission of the rights-holder. Note that no code of AmigaOS 4.x was released or distributed.

Hyperion Entertainment holds an exclusive, world-wide, perpetual source-code license to the intellectual property of AmigaOS 3.1 and additional content as documented in the publicly available settlement agreement between Hyperion Entertainment and Amiga, Inc. which has taken the form of a stipulated judgement.

Based on this license AmigaOS 4.x development was started in 2001 by Hyperion Entertainment using the AmigaOS 3.1 code as a basis and as the direct successor of what Commodore left behind in 1994. AmigaOS 4.x is an actively developed product on sale and still incorporates a substantial amount of AmigaOS 3.1 code.

While this would be already more than enough of a reason to care about the unauthorised disclosure and distribution, it is also the very same settlement agreement which made all of this possible in the first place, which contractually requires Hyperion to enforce and protect any intellectual property rights associated with AmigaOS including the AmigaOS 3.1 source-code.

This entails that Hyperion Entertainment will examine all possible legal action against any unauthorised source of or use of this material it is aware of. All of this leads up to the reason why we "make such a fuss" about code which is more than 20 years old by now. While the original leak seems to stem from someone outside of the active community, it is even more sad to see quite some of the remaining active users happily participate in distributing this unauthorised copy, compromising years of development work and all possible future versions of AmigaOS and therefore biting the hand that feeds them against all common sense and in blatant violation of copyright.

Having said that, our most special thanks go to all loyal customers, user groups, dealers, partners and all others who showed and continue to show their support to us. You are the reason why AmigaOS still exists, why it remains under active development and why we care.

Thank you, on behalf of Hyperion Entertainment, all associated developers, translators and testers.

Hyperion Entertainment CVBA
Tervurenlaan 34
1040 Brussels
Belgium

info@hyperion-entertainment.com

=~=~=~=

->In This Week’s Gaming Section - U.S. Supreme Court Agrees To Hear Microsoft Appeal in Xbox Case!
"""""""""""""""""""""""""""""" Grand Theft Auto Studio Head Calls It Quits

!

Snoop Dogg to Bill Gates: 'Fix Your S***'!
And much more!

=~=~=~=

->A-ONE's Game Console Industry News - The Latest Gaming News!
"""""""""""""""""""""""""""""""""""""

U.S. Supreme Court Agrees To Hear Microsoft Appeal in Xbox Case

The U.S. Supreme Court on Friday agreed to consider Microsoft Corp's bid to fend off class action claims by Xbox 360 owners who contend that the videogame console has a design defect that causes game discs to be gouged.

The court will review a March 2015 ruling by the 9th U.S. Circuit Court of Appeals on the question of whether a lower court decision denying class certification to the plaintiffs could be challenged.

Class action lawsuits can lead to larger damages or broader remedies than individual lawsuits that can be costly to pursue.

Microsoft has sold tens of millions of Xbox 360 consoles since their 2005 launch. But owners have claimed that the console's optical disc drive cannot withstand even small vibrations. They said this causes game discs to spin out of control and become scratched even under normal playing conditions, rendering them unplayable.

Microsoft said class certification was improper because just 0.4 percent of Xbox owners reported disc scratches, and that misuse was the cause.

In 2012, U.S. District Judge Ricardo Martinez in Seattle dismissed the class action claims. He relied on a 2009 ruling in a similar case in which another judge said the dearth of complaints ruled out class certification.

The case is Microsoft Corp v. Baker, U.S. Supreme Court, No. 15-457.

Grand Theft Auto Studio Head Calls It Quits

You may not be familiar with the man s name, but you probably know his work.

Leslie Benzies, the president of Grand Theft Auto developer Rockstar North, has departed the company after a 17-month sabbatical, reports Kotaku.

Born in Aberdeen, Scotland, Benzies came aboard Rockstar North predecessor DMA Design in 1999 as a game programmer. In 2001 he helped launch the seminal Grand Theft Auto III as the game s producer, bringing the then-obscure GTA franchise into the third dimension and into the world s spotlight. He went on to lead the development of all subsequent GTA games, and is credited as a lead designer on Rockstar s acclaimed Western-themed game, Red Dead Redemption.

The media-shy Benzies presided over a development studio known for its thoroughness and attention to detail. We don t just go, Here s a mission, off you go, Benzies said in a 2013 profile for Develop magazine. We spend a lot of time, make a lot of graphs and work out how difficult something is, what the reward is, how you might be feeling after that mission.

 That last five to ten per cent of work on the game makes a huge difference, Benzies insisted. This level of perfection is not seen or understood in the majority of the industry. We can all make a car drive down a street in a game, but can you do it in style?

That perfectionism paid off. For the past 15 years, Grand Theft Auto has been gaming s crown jewel, with each iteration garnering outrageous sales and critical acclaim despite outcry over its violent content. Benzies himself was honored in 2005 with a BAFTA Special Award and was inducted into the Academy of Arts and Sciences Hall of Fame in 2014.

Rockstar North veterans Aaron Garbut and Rob Nelson will helm the studio moving forward, but no one knows what Benzies is up to next. We d say he deserves a long vacation, but it looks like he s already in the middle of one.

Snoop Dogg to Bill Gates: ’Fix Your S***’

An Xbox Live outage on Wednesday miffed countless gamers including Snoop Dogg.

The obviously put-out rapper took to Instagram this week to address "Xbox One or Microsoft or whoever the f***." In a very NSFW video, Snoop bemoaned the disruption, threatening to replace his Microsoft console with a Sony PlayStation.

"Y’all f***ing server is f***ing wack, man," the rapper, actor, and entrepreneur said. "Y’all gonna make me switch to PlayStation if y’all don’t ever get this s*** fixed."

As of press time, the Instagram video had almost 40,000 likes, and a handful of encouraging comments. The same clip, reposted eight hours later with a black-and-white filter, received another 20,800 likes.

According to reports, the Xbox Live outage began around 2 p.m. Eastern, knocking party chat, online gaming, and other functions offline for Xbox One$333.61 at Amazon, Xbox 360, and Windows

users.

The issue was resolved before midnight, and Redmond’s Xbox Live Status page today shows all services running normally.

But the waiting is the hardest part and patience doesn’t appear to be Snoop Dogg’s strong suit. During his gaming downtime, the 44-year-old record exec went straight to the top, addressing Microsoft’s co-founder directly.

"What the f*** is you doin’, Bill Gates?" Snoop said at the end of the 15-second video. "Fix your s***, man."

Gates is a Microsoft co-founder, but is far from the public face of Xbox; that would be Phil Spencer. Microsoft did not immediately respond to PCMag’s request for comment.

Hideo Kojima Will Be Inducted Into Gaming Hall of Fame

The Academy of Interactive Arts and Sciences on Tuesday announced that Metal Gear Solid creator Hideo Kojima will become the 21st inductee to the organization’s Hall of Fame. He will accept the award in person during a ceremony at the 19th D.I.C.E. Awards in Las Vegas on February 18.

And who will present the award to Kojima?

None other than film director and writer Guillermo del Toro. Kojima and del Toro worked together on Silent Hills before its cancellation and are hoping to one day find their way back to each other for a future project.
2987067-kojima.jpg

"Hideo Kojima’s career-defining works have shaped much of how the video game industry approaches cinematic storytelling and player engagement," AIAS president Martin Rae said in a statement. "As one of the most well-loved and well-respected designers of our time, it is a great honor for the Academy to induct him into our Hall of Fame. Hideo is a game creator whose eyes have always looked towards the future, and we look forward to his thoughts on the D.I.C.E. Summit stage."

AIAS Hall of Fame status is given to game creators "who have been instrumental in the development of highly influential games and moving a particular genre forward. These individuals demonstrate the highest level of creativity and innovation, resulting in significant product influence on a scale that expands the scope of the industry."

Previous AIAS Hall of Fame inductees have included people like Leslie Benzies, Dan Houser, and Sam Houser of Rock Games, as well as Epic Games CEO Tim Sweeney, Valve’s Gabe Newell, and BioWare founders Greg Zeschuk and Ray Muzyka. Nintendo legend Shigeru Miyamoto was the first inductee, back in 1998.

Last month, Kojima left Konami after two decades with the Japanese publisher. He now runs his own studio in Japan, Kojima

Productions, and is working with Sony on a new PlayStation 4 and PC game.

"I want to create something that’s what people expect, but at the same time will have something new that people haven’t seen before," he explained in an interview last month.

=~=~=~=

->A-ONE Gaming Online - Online Users Growl & Purr!
"""""""""""""""""""""

Bandit Gaming: Mortal Kombat for the Atari 2600 Work in Progress

In the early 1990 s we saw the release of Street Fighter II a title that changed arcades till their last days. Midway couldn t stand idly by so they released a one on one fighting game that took things a few steps farther. While Street Fighter II was a cartoon style game like most arcade games of the time, Mortal Kombat came in with digitized graphics. Real actors portrayed the moves featured in the game while Street Fighter II used hand drawn animation. Now, nearly 20 years after its initial release, Mortal Kombat is coming to the Atari 2600.

This is not an official port, hence the title Bandit Gaming . Midway, or whomever owns the rights now, is not behind this game in any way that I know of. That would be cool if we could get some support for this like we saw with Halo 2600 and are seeing for Legend on Atari 2600. It could happen. It is just good old plain good support of the fanbase. No one is going to confuse this with the currently being sold games, not by any stretch of the imagination.

What is here is a two player battle with both players controlling Raiden. Don t expect fatalities just yet. Right now, the animation is pretty basic and it would be tough for a person that has no knowledge of Mortal Kombat to figure out that is Raiden. He is just a jumble of pixels at the moment. The Outlands are similarly displayed but well, this is the Atari 2600 so what can you really expect?

AtariAge forum member, Jinroh is working on Mortal Kombat for Atari 2600 in his spare time. He is putting as much time has he can into this work in progress so progress should be available in the not too distant future.

UPP! Homebrew Released for Atari 2600

To say that the Atari 2600 is dead is only half right. If you are talking about going to Walmart and buying games then yes, it is

dead. If you are a little more open minded and know where to look (around here at RGM is a good start) then you can find a plethora of new Atari 2600 games. For example, UPP! for the Atari 2600 is a new take on an old idea. If you have played, or remember, Breakout then you know the basics of UPP! The difference is, those basics are turned on their heads here.

The idea of Breakout holds true in UPP! except it is not you playing that classic. NO, here you are the ship on the playfield trying to avoid the iconic paddle and ball. While the game is playing out a game of Breakout you are controlling a spaceship that is trying to collect a power up that drops, rather lazily, from the top of the screen. I say lazily drops because that power up is in no way a hurry to get to your ship. Once you collect the power up some of the blocks disappear from the playfield. Beating a level requires enough blocks be gone so that you can pass through into the opening that drifts across the top of the screen.

Complicating matters are random laser shots from the bottom of the screen. Hitting those, or the ball, will cost you a life. UPP! is a quirky take on the classic Breakout premise, something expanding on the idea.

UPP! is made available on cartridge, available on Etsy, complete with box and manual. If you are more of a digital gamer, or wish to try before you pay too much, you can hit up the itch.io store. This is a great opportunity to try UPP! out, support an indie developer and help more titles be developed.

=~=~=~=

A-ONE's Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

Police Arrested Hackers Who Stole Millions from European ATMs

Romanian law enforcement authorities have arrested eight cyber criminals suspected of being part of an international criminal gang that pilfered cash from ATMs (automatic teller machines) using malware.

The operation said to be one of the first operations of this type in Europe, was conducted in Romania and Moldova by Romanian National Police and the Directorate for Investigating Organised Crimes and Terrorism (DIICOT), with assistance from Europol, Eurojust and other European law enforcement authorities.

Europol did not provide names of any of the eight criminals arrested but said that the gang allegedly used a piece of malware, dubbed Tyupkin, to conduct what are known as Jackpotting attacks and made millions by infecting ATMs across Europe and beyond.

With the help of Tyupkin malware, the suspects were able to empty cash from infected ATMs by issuing commands through the ATM’s pin pad.

"The criminal group was involved in large scale ATM Jackpotting a term which refers to the use of a Trojan horse, physically launched via an executable file in order to target an ATM," Europol explained in a press release, "thus allowing the attackers to empty the ATM cash cassettes via direct manipulation, using the ATM PIN pad to submit commands to the Trojan."

Tyupkin was first analysed in 2014 by Kaspersky Lab following the request from a financial institution. During the investigation, Kaspersky found the malware threat on more than 50 ATMs in Eastern Europe.

The malware allows its operators to withdraw cash from ATMs without the requirement of any payment card.

Although, Europol did not specify how much money in total the criminal gang was able to plunder, it believed that the gang was able to cause substantial losses across Europe and that the losses could be in Millions.

Cyber Attacks on Manufacturing Spiked Last Year

Department of Homeland Security investigations of cyber attacks on the nation’s critical manufacturing sector nearly doubled in the year ended Sept. 30, according to the agency.

The Department of Homeland Security’s Industrial Control Systems Cybersecurity Emergency Response Team, or ICS-CERT, said in a report distributed this week that it investigated 97 incidents at critical manufacturers during its most-recent fiscal year.

That category includes makers of vehicles and other types of transportation equipment as well as metals, machinery and electrical equipment producers.

ICS-CERT said that altogether it responded to a total of 295 cyber incidents, up 20 percent from the previous fiscal year. After critical manufacturing, the next most active sectors were energy, with 46 incidents, water, with 25, and transportation systems, with 23, according to the report. The document did not say whether any of the incidents caused outages or say who was behind them. A DHS spokesman declined to elaborate.

Cyber experts say that such incidents could be caused by unintentional infections of criminal malware, nations and criminals gathering data to prepare for potential destructive attacks in the future, or attacks looking to disrupt service.

Hackers Cause World’s First Power Outage with Malware

SCADA system has always been an interesting target for cyber crooks, given the success of Stuxnet malware that was developed by the US and Israeli together to sabotage the Iranian nuclear facilities a few years ago, and "Havex" that previously targeted organizations in the energy sector.

Now once again, hackers have used highly destructive malware and infected, at least, three regional power authorities in Ukraine, causing blackouts across the Ivano-Frankivsk region of Ukraine on 23rd December.

The energy ministry confirmed it was investigating claims a cyber attack disrupted local energy provider Prykarpattyaoblenergo, causing the power outage that left half of the homes in Ivano-Frankivsk without electricity just before Christmas.

According to a Ukrainian news service TSN, the outage was the result of nasty malware that disconnected electrical substations.

On Monday, researchers from antivirus provider ESET confirmed that multiple power authorities in Ukraine were infected by "BlackEnergy" trojan.

BlackEnergy Trojan was first discovered in 2007 as a relatively simple tool to conduct Distributed Denial of Service (DDoS) attacks but was updated two years ago to add a host of new features, including the ability to render infected computers unbootable.

The malware was launched by "Russian security services" with it being used against industrial control systems and politically sensitive targets, the SBU state intelligence service said in a statement on Monday.

According to ESET, the malware was recently updated again to add a new component called KillDisk and a backdoored secure shell (SSH) utility that gives hackers permanent access to infected computers.

The KillDisk module enables the BlackEnergy malware to destroy critical parts of a computer hard drive and to sabotage industrial control systems, the same used in attacks against Ukrainian news media companies and the electrical power industry.

"The first known case where the KillDisk component of BlackEnergy was used was documented by CERT-UA in November 2015," Anton Cherepanov of ESET wrote in a blog post. "In that instance, a number of news media companies were attacked at the time of the 2015 Ukrainian local elections. The report claims that a large number of video materials and various documents were destroyed as a result of the attack."

Researchers said hackers had used backdoors to spread the KillDisk wiper module through booby-trapped macro functions embedded in Microsoft Office documents across the Ukrainian power authorities.

Therefore, it is believed that the initial point of infection

with BlackEnergy caused after employees opened Microsoft Office files containing malicious macros.

It is really disturbing that industrial control systems used to supply power to Millions of homes could be infected using such a simple social-engineering trick.

Moreover, the most concerning part is that the BlackEnergy malware is now being used to create power failures that can even have life-and-death consequences for large numbers of people.

Ukrainian authorities are investigating the hacking attack on its power grid. For more technical details about the latest BlackEnergy package, you can read on ESET blog.

Plain Cruelty: Boffins Flay Linux Ransomware for The Third Time

Probably the world’s most tragically determined blackhat developers have had their revitalised Linux.Encoder ransomware pwned again by meddling BitDefender whitehats.

The third iteration of the Linux.Encoder ransomware was unleashed on the world, infecting a paltry 600 servers before a crack team of security analysts returned to rip it apart.

Once again, instead of paying the VXers a Bitcoin to fund training them out of hopelessness, victims can run BitDefender’s decryption utility to release their locked-up files free of charge.

Linux.Encoder’s defiant developers took lesson from the failings of the first and second versions which were ripped up days after release such that victims could decrypt their files for free, neutering the malware.

They even heeded Twitter invective from the sarcastic security swarm which proffered cryptographic clues about how they may improve their net nasty.

It was not enough, according to BitDefender boffin Radu Caragea.

"As we expected, the creators of Linux.Encoder have fixed their previous bugs and have come up with a new and improved variant," Caragea says.

"Luckily for the victims, the new variant of Linux.Encoder is still vulnerable to key recovery attacks."

Bitdefender highlighted that in earlier versions file modification time could be used to work out the ransomware’s random key generation and to reverse the encryption.

Twitter scoffed, pointing out that the method is insecure and should be altered.

"Apparently, the operators actually took note of these sarcastic recommendations; as a result, the IV (initialisation vector) is

now generated from a hash of the file size and the filename 32 bytes from rand() are hashed 8 times and used as the AES-256 key," Caragea says.

And the attackers still made n00b-level coding errors. For example, there's a missing static link in the libc library that stops the ransomware launching on older systems that would be easier to pwn.

Caragea called the last Linux.Encoder variant a counterstrike a "close shave" and says victims who escape the grasp of the third version may not get a fourth chance.

"While this is the third lucky strike, please make sure that, after recovery, you update the vulnerable platforms and stop this type of attack cold in the first place."

"Next time, hackers could actually come up with a working version of the ransomware that won t be as easy to decrypt."

Creator of MegalodonHTTP DDoS Botnet Arrested

Last month, the Norway police arrested five hackers accused of running the MegalodonHTTP Remote Access Trojan (RAT).

The arrests came as part of the joint operation between Norway s Kripos National Criminal Investigation Service and Europol, codenamed "OP Falling sTAR."

According to the United States security firm, all the five men, aged between 16 and 24 years and located in Romania, France, and Norway, were charged with possessing, using and selling malware.

One of those arrested also confessed to running his own web store where he sold malware, designed to take full control of target computers, harvesting passwords, and other personal data.

Moreover, the malware can be used to hijack webcams in real-time, and steal documents, images, and videos as well.

"Damballa's threat discovery center worked in cooperation with the Norway police over the last few months to track and identify the author of the malware dubbed MegalodonHTTP," threat researcher Loucif Kharouni wrote in a blog post.

"We are not at liberty to divulge the MegalodonHTTP author s real identity, but we can confirm that the person behind the handle Bin4ry is no longer active or doing business."

However, the researchers said MegalodonHTTP was not very powerful; in fact, it was "quite simple" and indicated the poor coding skills of its author, requiring .NET to be installed on infected systems.

MegalodonHTTP included a number of features as listed below:

Binary downloading and executing

Distributed Denial of service (DDoS) attack methods
Remote shell
Antivirus Disabling
Crypto miner for Bitcoin, Litecoin, Omnicoin and Dogecoin

However, MegalodonHTTP is not an advanced malware, according to the researchers, and its author wanted to develop modular malware with a number of malicious features, but remained "as small as possible, around 20Kb."

This malware was sold on amateur hacker hangout HackForum as well as on the bin4ry[dot]com website. In fact, before his arrest last month, the hacker was still selling the malware.

Just last week, Europol in cooperation with Romanian law enforcement authorities arrested eight criminal hackers suspected of being part of an international criminal gang that pilfered cash from ATMs using malware.

602 Gbps! This May Have Been the Largest DDoS Attack in History

Cyber attacks are getting evil and worst nightmare for companies day-by-day, and the Distributed Denial of Service (DDoS) attack is one of the favorite weapon for hackers to temporarily suspend services of a host connected to the Internet.

Until now, nearly every big website had been a victim of this attack, and the most recent one was conducted against the BBC’s websites and Republican presidential candidate Donald Trump’s main campaign website over this past holiday weekend.

Out of two, the largest DDoS attack in the history was carried out against the BBC website: Over 600 Gbps.

The group calling itself New World Hacking claimed responsibility for taking down both the BBC’s global website and Donald Trump’s website last week.

The group targeted all BBC sites, including its iPlayer on-demand service, and took them down for at least three hours on New Year’s Eve.

At the moment, the BBC news organization announced that the outage was caused due to some "technical" fault, but later it stated that "New World Hacking" group had claimed responsibility for launching a DDoS attack against BBC, as a "test of its capabilities."

One of the members of the New World Hacking group, identified himself as Ownz, claimed that the group allegedly used their own tool called BangStresser to launch a DDoS attack of up to 602 Gbps on the BBC’s website.

As a proof, the group provided ZDNet a screenshot of a web interface that was allegedly used to attack the BBC website.

Although the authenticity of the screenshot has not been verified,

if the attack size is proven true, it would vastly surpass the largest DDoS attack record of 334 Gbps, recorded by Arbor Networks last year.

The recent massive DDoS attack apparently utilizes two Amazon Web Services servers that employ a large number of automated detection and mitigation techniques in order to prevent the misuse of the services, Amazon previously claimed.

"We have our ways of bypassing Amazon," said Ownz. "The best way to describe it is we tap into a few administrative services that Amazon is use to using. The [sic] simply set our bandwidth limit as unlimited and program our own scripts to hide it."

More details about the attack have yet not disclosed, but Ownz claimed that their main purpose behind the development of the BangStresser DDoS tool is to unmask ISIS and possibly end its online propaganda.

"We have been taking down ISIS websites in the past," said Ownz, "this is just the start of a new year."

A similar group named Lizard Squad, conducted a marketing campaign for promoting their DDoS tool, known as the Lizard Stresser, using which the group took down Sony's PlayStation Network and Microsoft's Xbox Live last year on Christmas Eve.

Trend Micro Anti-virus Software Leaves Users Open to Attack

When they're not working on their own projects, Google engineers often focus on highlighting potential issues with software delivered by others. We've already seen bug hunter Tavis Ormandy expose a vulnerability in AVG's Chrome security add-on, but he's now also found an exploit in another popular virus scanner: Trend Micro.

According to Ormandy's security disclosure, a weakness in Trend Micro's Password Manager, which is automatically installed alongside the main scanner on Windows machines, let attackers execute commands and launch programs on unsuspecting users' PCs. He also pointed out that all saved passwords on the machine could be read as a result.

The company is said to have used an old API that invoked an "ancient" build of Chromium (the engine that powers Google's Chrome browser). We're currently up to version 49, but the security company utilized version 41, which dates back to January 2015. Using this, the program would break out of its sandbox, an environment designed to stop attackers from being able to access areas they shouldn't, in order to offer a "secure browser" to users. In the example below, the Google engineer was able to run a local program, Windows Calculator in this case, but it could also be used to execute a remote attack.

"I don't even know what to say - how could you enable this thing *by default* on all your customer machines without getting an audit from a competent security consultant?," says Ormandy.

The disclosure also highlights a worrying trend (I know, I know): security companies that provide additional tools to protect people from malicious attacks are actually putting them more at risk. Plus, users may never know that their computer has been attacked.

Trend Micro says it moved quickly to patch the vulnerabilities and "worked with Tavis throughout the process" to resolve them. "Thanks to his responsible work with us, we were able to address the most critical issues he brought us in less than one week."

Trend Micro Patches Password Manager Bug

Trend Micro’s Password Manager has come under fire for potentially allowing a malicious website to run arbitrary code on a computer.

Earlier this month, security researcher Tavis Ormandy discovered a security flaw in Trend Micro’s Password Manager. According to a post on Google’s Security Research site, when users installed Trend Micro Antivirus on Windows, a Password Manager app downloaded automatically, too. Unfortunately that app used an "ancient build of Chromium" that left it open to attacks and, ironically, put people’s passwords at risk.

"It took about 30 seconds to spot [an API] that permits arbitrary command execution," Ormandy wrote last week. "This means any website can launch arbitrary commands."

On Monday, Trend Micro said it addressed the issue through a mandatory update. It did not appear that anyone had exploited it, said Christopher Budd from Trend Micro’s Global Threat Communications team.

"As part of our standard investigation we checked and verified that the only product affected by these issues is our consumer Trend Micro Password Manager and no commercial or enterprise products are affected," Budd said. "We released a mandatory update through Trend Micro’s ActiveUpdate technology on January 11, 2016 that fixes these problems: all customers should have that now."

Last month, Ormandy discovered a bug within AVG Web TuneUp that put the info of 9 million users at risk.

Microsoft Fixes Critical Flaws in Windows, Office, Edge, IE and Other Products

Microsoft has released the first batch of security updates for 2016 and they include critical fixes for remote code execution flaws in Windows, Office, Edge, Internet Explorer, Silverlight and Visual Basic.

The company has also fixed remote code execution and elevation of

privilege vulnerabilities in Windows and an address spoofing flaw in Exchange Server, that were rated important, not critical, due to various mitigating factors.

In total, Microsoft issued nine security bulletins covering patches for 24 vulnerabilities.

According to Wolfgang Kandek, the CTO of security firm Qualys, administrators should prioritize the MS16-005 security bulletin, especially for systems running Windows Vista, 7 and Server 2008.

This patch addresses a remote code execution vulnerability tracked as CVE-2016-0009 that has been publicly disclosed, making attacks more likely.

The second most important bulletin, according to Qualys, is MS16-004, which addresses six vulnerabilities in Microsoft Office. This bulletin is rated critical, which has been unusual for Microsoft Office in the recent past.

The culprit for this severity rating is one particular remote code execution vulnerability tracked as CVE-2016-0010 that’s present in all versions of Office from 2007 to 2016, even those running on Mac and Windows RT, Kandek said in a blog post.

Researchers from security firm Tripwire believe that the Internet Explorer and Microsoft Edge patches should be at the top of the priority list instead, because they address vulnerabilities that could be remotely exploited through malicious or compromised websites.

These patches are covered in the MS16-001 and MS16-002 security bulletins and will be the last ones that Internet Explorer versions 8 and 10 will ever receive. IE 9 will continue to be supported on Windows Vista and Windows Server 2008 SP2.

"Many enterprises need to use older versions of IE within their environments because of very expensive, legacy web applications that use outdated technology," said Lane Thames, security researcher at Tripwire, via email. "Organizations who still depend on legacy applications that require these older IE versions will need to move appropriately."

Companies that use Outlook Web Access (OWA) should also prioritize MS16-010. Even though this bulletin is rated by Microsoft only as important, the vulnerability it covers can allow attackers to launch so-called business e-mail compromise (BEC) attacks.

Such attacks have cost companies around the world $1.2 billion, according to statistics published in August by the FBI’s Internet Crime Complaint Center (IC3). It involves attackers compromising business emails, or spoofing email addresses, to instruct employees and business partners to initiate unauthorized wire transfers.

Finally, the MS16-006 bulletin, which addresses a vulnerability in Silverlight, should be on the priority list as well because the flaw could enable remote code execution attacks through the browser plug-in. Attackers are known to have used Silverlight

exploits in the past.

This month’s updates were also the last ones for Windows 8, which Microsoft will no longer support going forward. Windows 8 users will have to upgrade to Windows 8.1 or 10 in order to continue receiving security patches.

Gatekeeper Flaw Remains Exploitable Four Months After Its Discovery

A security researcher says flaws in Apple s Gatekeeper application validation system remain available to exploit, despite Apple patching some vectors he disclosed on September 30 in security updates released in November and December.

It took me literally five minutes to completely bypass, says Patrick Wardle, director of research at Synack. He s not just talking about the problem: He s also released a tool to block the unpatched pathways to exploitation. To make use of this flaw, a legitimate app has to be modified by a malicious party and then distributed or swapped in when a user thinks the correct package is being downloaded. That said, it remains a reasonable concern.

An Apple spokesperson tells Macworld that it has added the latest specific unsigned app components identified by Wardle to its XProtect list, preventing their launch, and has engaged in productive discussions. The company says it continues to work on improving the security of Gatekeeper.

Apple designed Gatekeeper to provide a heightened level of integrity around Mac apps from registered developers without restricting all downloads to the Mac App Store. With the Security & Privacy system preference pane s Allows Apps Downloaded From set to Mac App Store and Identified Developers, only apps in that latter category that have been cryptographically signed by a certificate issued by Apple should launch, and only after given the prompt that you re launching software that was downloaded from the Internet.

Wardle s September disclosure stated that while Apple examined the digital signature on the binary executable the compiled software at the core of the downloaded package Gatekeeper didn t check other software in the package that could be executed by that binary. Wardle easily found downloadable apps from major vendors where he could swap out modules for malicious code, and Gatekeeper wouldn t squawk. It s important to note that these apps aren t malicious, and don t even follow poor programming guidelines. They re legitimate, developer-signed OS X apps that can be tinkered with to add a malicious payload.

Macworld spoke with Wardle a few days before his updated presentation at the ShmooCon security conference on January 15, and he explained that Apple s patches last year for his first disclosures were very thin: Rather than comprehensively fix the problem of downloaded executables, Apple blocked one vector (related to dynamic libraries) and blocked specific apps that could be subverted. Wardle reported all of this to Apple, and says they are going to be releasing an update to patch this,

but all they re going to do is blacklist the new binary I found. (Apple confirms the blacklisting has already occurred.)

He also remains convinced that Gatekeeper should more broadly inspect software before first launch, not just the subset that it currently examines. In his presentation, he notes that non-Apple software that downloads files from the Internet including torrenting apps don t all mark these files with a quarantine attribute that triggers examining the Security & Privacy settings to determine what to do about it and, if it meets criteria, shows the warning that a file was downloaded and asks for your approval before proceeding.

Because Gatekeeper ignores these files, any apps downloaded in this manner bypass Gatekeeper. Malware that s already on a system can also download executables that won t trigger a warning. (Apple s automatically updated XProtect library of malware signatures will still prevent specific software from launching.)

This Gatekeeper flaw still requires a big if : You have to download, install, and choose to launch software that s been tampered with. That should be difficult, but there remain three ways to ne er-do-wells to insert themselves as men-in-the-middle (MitM) and swap out a legitimate download for a maliciously modified one:

The developer s site could be hacked, and a new download put in place that appears to be identical to the previous one. That s always a possibility, but because Gatekeeper wouldn t warn users downloading a suborned package, it could go unnoticed for some time. (In the Unix world, hosted files are paired with cryptographic signatures that allow a downloader to confirm the retrieved package is the one the developer distributed.)

A developer that offers downloads via http (unsecured web connections) allows an MitM at a favorable network location to swap in a modified package undetectably. Wardle says many, many OS security software vendors (not to mention those making other kinds of software) don t use SSL/TLS over https. There s no excuse for this, as there s almost zero cost and no technical reason at this point to use secured web connections for downloads. (A new effort called Let s Encrypt even allows the free creation of server certificates.)

A user downloads software from a third-party downloads or updates site. I strongly urge you to never download OS X software from anywhere except from a developer s own site or the Mac App Store.

Wardle says Apple told him that it s working on a more comprehensive fix, and Apple confirmed without any details that it continues to improve Gatekeeper. Until a more thoroughly preventative update is available, Wardle has released a new tool called Ostiarius that when installed prevents the launch of any unsigned program that hasn t been specifically approved by you already.

As a long-time Apple user, Wardle remains frustrated that Apple has put partial measures in place. Because of this, he says

attackers can look at Apple s security release notes to reverse engineer what the company fixed, and see if they failed to repair it comprehensively. Apple isn t as proactive or aggressive about security as they should be, he says.

ProPublica Launches The Dark Web s First Major News Site

The so-called dark web, for all its notoriety as a haven for criminals and drug dealers, is slowly starting to look more and more like a more privacy-preserving mirror of the web as a whole. Now it s gained one more upstanding member: the non-profit news organization ProPublica.

On Wednesday, ProPublica became the first known major media outlet to launch a version of its site that runs as a hidden service on the Tor network, the anonymity system that powers the thousands of untraceable websites that are sometimes known as the darknet or dark web. The move, ProPublica says, is designed to offer the best possible privacy protections for its visitors seeking to read the site s news with their anonymity fully intact. Unlike mere SSL encryption, which hides the content of the site a web visitor is accessing, the Tor hidden service would ensure that even the fact that the reader visited ProPublica s website would be hidden from an eavesdropper or Internet service provider.

 Everyone should have the ability to decide what types of metadata they leave behind, says Mike Tigas, ProPublica s developer who worked on the Tor hidden service. We don t want anyone to know that you came to us or what you read.

Of course, any privacy-conscious user can achieve a very similar level of anonymity by simply visiting ProPublica s regular site through their Tor Browser. But as Tigas points out, that approach does leave the reader open to the risk of a malicious exit node, the computer in Tor s network of volunteer proxies that makes the final connection to the destination site. If the anonymous user connects to a part of ProPublica that isn t SSL-encrypted most of the site runs SSL, but not yet every page then the malicious relay could read what the user is viewing. Or even on SSL-encrypted pages, the exit node could simply see that the user was visiting ProPublica. When a Tor user visits ProPublica s Tor hidden service, by contrast and the hidden service can only be accessed when the visitor runs Tor the traffic stays under the cloak of Tor s anonymity all the way to ProPublica s server.

Tigas first began considering launching a hidden service last year when the news site was working on a report about Chinese online censorship and wanted to make sure the reporting was itself safe to visit for Chinese readers.

To most of ProPublica s readers, that no doubt sounds like an unnecessary level of paranoia to go through to read the news. But Tigas first began considering launching a hidden service last year when the news site was working on a report about Chinese online censorship and wanted to make sure the reporting was itself safe to visit for Chinese readers. Like other news sites, ProPublica also accepts anonymous tips and leaks through its

SecureDrop server, another Tor hidden service. Tigas says he hopes the Tor hidden service version of the site will make sure any leaker can also read the stories resulting from those leaks with as much protection as possible. It remains to be seen how readers will find the new Tor hidden service, as ProPublica hasn t yet decided where it will advertise it. The launch makes Pro Publica the first major media site on the dark web, but not the first news site altogether. The dark web news site Deep Dot Web has long hosted a hidden service version of itself for its privacy-focused readers.

Tor hidden services, which hide the IP address of a web site and thus its administrator s identity, have been widely used for online narcotics sales like the Silk Road and even child pornography. But ProPublica s dark web site is far from the first foray from reputable publishers and web companies into Tor s anonymity network. In late 2014, Facebook launched its own Tor hidden service. (Though Facebook itself knows the identity of any user who logs into that Tor-enabled mirror of the site, eavesdroppers wouldn t.) Media sites including the Guardian, the Intercept, and the New Yorker have the software SecureDrop to launch WikiLeaks-style anonymous upload sites on the dark web. And a variety of apps are beginning to use Tor hidden services, too, like the anonymous chat service Ricochet and the file-sharing service Onionshare.

ProPublica s Tigas says he hopes the news site s hidden service will serve as a model for other media companies who want to protect users privacy, and maybe improve the dark web s controversial reputation, too. Personally I hope other people see that there are uses for hidden services that aren t just hosting illegal sites, Tigas says. Having good examples of sites like ProPublica and Securedrop using hidden services shows that these things aren t just for criminals.

Microsoft Collecting More Data of Windows 10 Users Than Initially Thought

After several controversial data mining and privacy invasion features within Microsoft’s newest operating system, Microsoft continued convincing its users that Windows 10 is not spying on anyone and that the company is not collecting more data than it needs.

In addition, Microsoft also updated its privacy policy in order to clear how and when Windows 10 utilizes users’ data.

But wait, before you convinced yourself by this statement, just have a look on the milestones (listed below) that Microsoft recently announced, revealing that Windows 10 is now actively running on 200 Million devices.

Here’s the list of milestones that Microsoft just achieved:

- People spent over 11 Billion hours on Windows 10 in December 2015.
- More than 44.5 Billion minutes were spent in Microsoft Edge

across Windows 10 devices in December alone.
Windows 10 users asked Cortana over 2.5 Billion questions since launch.
About 30 percent more Bing search queries per Windows 10 device compared to prior versions of Windows.
Over 82 Billion photographs were viewed in the Windows 10 Photo application.
Gamers spent more than 4 Billion hours playing PC games on Windows 10 OS.
Gamers streamed more than 6.6 Million hours of Xbox One games to Windows 10 PCs.

Maybe Microsoft listed these statistics in order to illustrate just how popular its newest operating system has become, but what the company missed is:

Microsoft itself admitted that how deeply it is tracking Windows 10 users.

First noticed by Martin Brinkmann of gHacks, these statistics clearly indicate that Microsoft is not only keeping itself updated about the Windows 10 installation on different devices but is also tracking every single activity of its users by collecting more data than initially thought.

Playing a game? Microsoft tracks it.

Asking Cortana a question? Microsoft tracks it.

Opening Edge browser? Microsoft tracks it, too.

"While it is unclear what data is exactly collected," Brinkmann says, "it is clear that the company is collecting information about the use of individual applications and programs on Windows at the very least."

This is the actual dirty side of the free Windows 10 upgrade that we many times talk about, and with time, it will be more shocking to you because the most worrisome part of Windows 10 is that there’s no easy way to turn this data collection off.

How Do Americans Feel About Sharing Personal Info? ’It Depends’

While many are willing to share personal details in exchange for benefits, they are often unhappy about what happens to that information once collected.

At what point does it become too risky to share you personal information? A drugstore loyalty card? Targeted online ads? According to a new Pew Research Center report, a majority of Americans consider security a trade-off.

"While many Americans are willing to share personal information in exchange for tangible benefits, they are often cautious about disclosing their information and frequently unhappy about what happens to that information once companies have collected it," Pew found.

More than 50 percent of people, for example, said it’s okay for their employer to install cameras in the office after a rash of workplace thefts. Nearly as many accept that retailers track their purchases with the promise of occasional discounts offered by loyalty cards.

But when Pew proposed saving money on energy bills by installing a smart thermostat that also monitors folks’ movements around the house, most adults considered this unacceptable.

"There will be no ’SMART’ anythings in this household," one respondent said. "I have enough personal data being stolen by the government and sold [by companies] to spammers now."

Web users also hate the unsolicited emails, phone calls, and customized ads they receive after sharing a piece of personal information on the Web.

"I want control over what ads are being ’pushed back’ to me: I have no interest in ’puppy portraits’ but I may be interested in cameras, equipment, etc.," one person told Pew. "In an effort to ’target’ my preferences, my inbox gets full of [expletive] that is not relevant to me."

A number of high-profile data breaches also seem to have left a bad taste in people’s mouths.

"These findings suggest that the phrase that best captures Americans’ views on the choice between privacy vs. disclosure of personal information is, ’It depends,’" said Pew Research Director of Internet, Science and Technology Lee Rainie and research associate Maeve Duggan.

It depends on the organizations with which they are sharing information. It depends on what happens to their data once it’s collected. It depends on how long those details are retained.

Pew surveyed 461 U.S. adults and nine online focus groups, presenting folks with six hypothetical scenarios, each involving sharing some level of personal data in exchange for using a product or service.

Seagate Unveils 10TB Helium Enterprise Drive To Address Storage Demands of Cloud-based Data Centers

Seagate Technology plc, a world leader in storage solutions, today launched its first 10TB enterprise capacity hard disk drive (HDD), merging high capacity with the industry s lowest power and weight available in a 10TB drive, to meet the growing storage requirements for private and public cloud-based data centers. The Seagatefi Enterprise 3.5 Capacity HDD has been selected by enterprise market leaders globally for its ability to address storage demands unlike any other technology in the industry.

Cloud-based data center storage needs are expanding faster than many current infrastructures can sustain, rendering the capacity

demands of users a herculean task for cloud managers, said Mark Re, senior vice president and chief technology officer, Seagate. Built on our years of research and development of sealed-drive technology, our new helium-based enterprise drive is designed precisely to help data-centric organizations worldwide solve the needs of their growing storage business.

With the amount of data today growing at an increasingly rapid rate, we are always on the lookout for storage solutions that offer better performance with lower overhead, said Fan Ruiqi, president of storage products at Huawei. The new Enterprise Capacity 3.5 HDD from Seagate helps us meet these demands by offering incredible capacity with improvements in power and weight allowing us to drastically reduce our costs.

The new, robust 10TB Enterprise Capacity 3.5 HDD provides maximum storage capacity for easy system integration by using the standard 3.5-inch CMR design. Incorporating seven platters and 14 heads, the drive seals in helium to create a turbulence-free, quiet environment, decreasing both friction and resistance on the platters and delivering the industry s lowest power/TB ratio and weight specifications for a 10TB HDD. Offering 25 percent more density to help businesses dramatically increase petabytes per rack, the drive delivers higher performance and reduced power and weight.

More and more data centers are being put into operation as a result of data growing at an exponential rate. With this in mind, we are laser focused on lowering our TCO and confident the new Seagate Enterprise Capacity 3.5 HDD can help us with this endeavor, said Li Shu, senior expert technical support for storage and research and development, at Alibaba. We value the drives winning combination of higher storage capacities, increased performance and low power consumption making it a win-win for both us and our customers.

At-scale data centers are faced with the challenge of efficiently storing massive amounts of unstructured digital data, said John Rydning, IDC s research vice president for hard disk drives. Seagate s new 10TB HDD for enterprise data centers is its first product to employ helium technology and will help data center customers to expand storage capacity economically.

The Enterprise Capacity 3.5 HDD improves performance by using advanced caching algorithms to help cloud data center managers manage the increasing volume of data more quickly. Featuring Seagate s PowerChoice technology, the drive helps businesses manage and reduce the ongoing costs associated with power and cooling during idle time, while Seagate s PowerBalance feature helps optimize the IOPS/Watt for even more efficiency.

It delivers an improved MTBF of 2.5 million hours and provides consistent performance to customers in a 24x7 multi-drive environment. Enterprise ready, the Seagate Enterprise Capacity 3.5 HDD is available in both a 6Gb/s SATA and 12Gb/s SAS interfaces.

The new Seagate Enterprise Capacity 3.5 HDD 10TB is now shipping to select customers worldwide. For more information on all Seagate products please visit www.seagate.com.

=~=~=~=

Atari Online News, Etc. is a weekly publication covering the entire Atari community. Reprint permission is granted, unless otherwise noted at the beginning of any article, to Atari user groups and not for profit publications only under the following terms: articles must remain unedited and include the issue number and author at the top of each article reprinted. Other reprints granted upon approval of request. Send requests to: dpj@atarinews.org

No issue of Atari Online News, Etc. may be included on any commercial media, nor uploaded or transmitted to any commercial online service or internet site, in whole or in part, by any agent or means, without the expressed consent or permission from the Publisher or Editor of Atari Online News, Etc.

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.